IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of   Atty. Docket

HUIBERT DEN BOER   PHN 15-813B

Serial No.   Group Art Unit:

Filed: CONCURRENTLY   Examiner:

Title: CRYPTOGRAPHIC METHOD AND APPARATUS FOR NON-LINEARLY MERGING A DATA BLOCK AND A KEY

Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Concurrent with the filing of this application and responsive to the Advisory Action mailed March 20, 2001 and the Final Office Action mailed September 12, 2000 with regard to a priority patent application, please amend the above-identified application as follows:

IN THE SPECIFICATION

Page 1, in the paragraph beginning on line 1, change as follows:

FIELD OF THE INVENTION

The invention relates to a method for converting a digital input block into a digital output block; said conversion comprising the step of merging a selected part M1 of the digital input block with a first key K1 and producing a data block B1 which non-linearly depends on the selected part M1 and the first key K1, and where a selected part of the digital output block is derived from the data block B1.

Page 1, in the paragraph beginning on line 6, change as follows:

The invention further relates to an apparatus for cryptographically converting a digital input block into a digital output block; the apparatus comprising first input means for supplying the digital input block; second input means for supplying a first key K1; cryptographic processing means for converting the digital input block into the digital output block; such conversion comprising merging a selected part M1 of the digital input block with the first key K1 and producing a data block B1 which non-linearly depends on the selected part M1 and the first key K1, and where a selected part of the digital output block is derived from the data block B1; and output means for outputting the digital output block.

Page 1, in the paragraph beginning on line 15, change as follows:

BACKGROUND OF THE INVENTION

The Data Encryption Standard (DES) of the National Bureau of Standard [FIPS publication 46, 1977 January 15] describes a widely used algorithm for converting a digital input block into a digital output block. Such an algorithm is generally referred to as a block cipher. The DES algorithm is used for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting converts intelligible data, referred to as plaintext, into an unintelligible form, referred to as ciphertext. Decrypting the ciphertext converts the data back to its original form. In the so-called electronic code book mode, DES is used to encrypt blocks of 64 bits of plaintext into corresponding blocks of 64 bits of ciphertext. In this mode, the encryption uses keys which are derived from a 64 bit key, of which 56 bits may be freely selected. Figure 1 shows the overall structure of DES during encrypting. In the encrypting computation, the input (64 bit plaintext) is first permuted using a 64 bit fixed permutation IP. The result is split into 32 left bits L_0 and 32 right bits R_0. The right bits are transformed using a cipher function $f(R_0,K_1)$, where K_1 is a sub-key. The result $f(R_0,K_1)$ is added (bit-wise modulo 2) to the left bits, followed by interchanging the two resulting 32 bit blocks $L_0 \square f(R_0,K_1)$ and R_0. This procedure is continued iteratively for a total of 16 rounds. At the end of the last round the inverse permutation of the initial permutation IP is applied.

Page 3, in the paragraph beginning on line 6, change as follows:

SUMMARY OF THE INVENTION

It is an object of the invention to provide a cryptographic method and apparatus of the kind set forth which is more robust against cryptanalytic attacks.

Page 3, in the paragraph beginning on line 9, change as follows:

To achieve this object, the cryptographic method according to the invention is characterised in that the step of merging the data and the key is performed by executing a non-linear function g for non-linearly merging said selected part M1 of the data and said first key K1 in one, sequentially inseparable step. In the DES system, as shown in figure 2, in a first processing step the R data is bit-wise added to the key, followed by a second processing step of non-linearly processing the result (S-boxes). According to the invention, an algorithm is used which non-linearly merges data with a key in one step (i.e. one, sequentially inseparable step). As such, adding the key bits to the data is an integrated part of the non-linear operation, making the system more immune against modern attacks, such as differential cryptanalysis.

Page 3, in the paragraph beginning on line 19, change as follows:

In an embodiment of the method according to the invention , in each round both parts of the digital input block are processed, giving a better encryption result than for conventional Feistel ciphers, such as DES, where during each round only half of the digital input block is being processed. To ensure that the same system can be used for both encryption and decryption, one part of the data is processed using an operation g, whereas the other half is processed using the inverse operation g^{-1}. Using this scheme, decrypting is performed by using the same system but supplying the keys in reverse order to the rounds (during decryption the first non-linear step is supplied with the key which, during encryption, was supplied to the last non-linear step, etc). Compared to a conventional implementation of a Feistel cipher with twice as many rounds, the system according to the invention is faster.

Page 3, in the paragraph beginning on line 30, change as follows:

The measure of splitting a relatively large data block and key, of for instance 64 bits, into smaller sub-blocks and sub-keys simplifies real-time non-linear processing.

Page 3, in the paragraph beginning on line 33, change as follows:

In an embodiment of the method according to the invention , a constant is used to enhance the quality of the encryption. Advantageously, the constant is predetermined per system, forming, for instance, a customer-specific constant. Alternatively, the constant is generated using a pseudo-random generator.

Page 4, in the paragraph beginning on line 3, change as follows:

The invention provides a way for non-linearly merging the data sub-block and the sub-key in one step. Additionally, different inputs all result in different outputs. This increases the immunity of the system against cryptanalytic attacks, compared to DES where the non-linear operation reduces the 6-bit input sub-block to a 4-bit output sub-block, implying that the same output is produced for four different inputs.

Page 4, in the paragraph beginning on line 8, change as follows:

In an embodiment of the method according to the invention a constant is used to enhance the quality of the encryption. Advantageously, the constant is predetermined per system, forming, for instance, a customer-specific constant. Alternatively, the constant is generated using a pseudo-random generator.

Page 4, please delete the entire paragraph beginning on line 12.

Page 4, in the paragraph beginning on line 14, change as follows:

In an embodiment of the method according to the invention individual sub-blocks corresponding to different parts of the digital input block are swapped to improve the quality of the encryption.

Page 4, in the paragraph beginning on line 20, change as follows:

Another embodiment has the advantage of reducing the multiplication in GF(2^8) to operations in GF(2^4), making it possible to achieve a simpler or more cost-effective implementation.

Page 4, in the paragraph beginning on line 23, change as follows:

The multiplication in GF(2^8) may be reduced to operations in GF(2^4).

Page 4, in the paragraph beginning on line 28, change as follows:

An embodiment of the method according to the invention is characterised in that calculating the inverse b in an element of GF(2^8) comprises performing a series of calculations in GF(2^4). By reducing the inverse operation in GF(2^8) to operations in GF(2^4) a simpler or more-cost effective implementation can be achieved.

Page 5, in the paragraph beginning on line 13, change as follows:

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows the processing steps for the DES system,

Figure 2 illustrates details of merging the data with the key and the non-linear operation in DES,

Figure 3 illustrates details of the key calculation in DES,

Figure 4 shows a block diagram of the cryptographic apparatus of the invention,

Figure 5 illustrates separate processing of two parts of the digital input block,

Figure 6 illustrates processing of a part of the digital input block in the form of sub-blocks, Figure 7 illustrates processing of two parts in the form of sub-blocks, and

Figure 8 shows an overall encryption system.

Page 5, in the paragraph beginning on line 25, change as follows:

DETAILED DESCRIPTION OF THE INVENTION

Figure 4 shows a block diagram of the cryptographic apparatus 400 according to the invention. For the purpose of explaining the invention, the system is described in the electronic code book mode. Persons skilled in the art will be able to use the system in other modes as well.The apparatus 400 comprises first input means 410 for providing a digital input block M. The digital input block M may be any suitable size. Preferably, M is sufficiently large, for instance 128 bits, to obtain a reasonably secure encryption result. The apparatus 400 further comprises cryptographic processing means 420 for converting the digital input block into a digital output block. Advantageously, the digital output block has substantially equal length as the digital input block. The apparatus 400 comprises output means 430 for outputting the digital output block. Basically, the cryptographic processing means 420 converts the digital input block M into the digital output block by merging a selected part M1 of the digital input block M with a first key K1, producing a data block B1 which non-linearly depends on M1 and K1. The merging is performed in one, sequentially inseparable step. The digital output block is derived from B1 and the remaining part of M, which is not part of M1. To obtain the first key K1, the cryptographic apparatus 400 comprises second input block 440. As will be described in more details below, a second part M2 of the digital input block may be non-linearly merged with a second key K2, preferably, using an operation inverse to the operation for merging M1 and K1, producing a data block B2. In this case, the digital output block also depends on B2. To obtain the second key K2, the cryptographic apparatus 400 comprises third input block 450.

Page 6, in the paragraph beginning on line 22, change as follows:

Details of the cryptographic conversion process will now be described for encrypting blocks of 128 bits of plaintext into corresponding blocks of 128 bits of ciphertext. Persons skilled in the art will be able to use the system for other block sizes as well. Data sizes shown in the Figures are given for reasons of clarity and should be treated as examples only. The description focuses on the non-linear processing of the data and the merging of the key with the data as performed in one round. As such the invention can be applied in a system as shown in Figure 1, comprising multiple rounds and also including a linear operation on the data block in each round.

Page 10, in the paragraph beginning on line 19, change as follows:

In principle, for the invention any multiplication in GF(2^8) may be used. An example of a VLSI implementation of multiplications in GF(2^m) is given in [P. A. Scott, "A fast VLSI multiplier for GF(2^m)", IEEE Journal on selected areas in communications, Vol. SAC-4, No. 1, January 1986, pages 62-66]. Advantageously, the following mechanism is used to reduce the multiplication in GF(2^8) to a series of multiplications and additions in GF(2^4). As is known in the art, in finite fields with a characteristic of 2 (e.g. GF(2^n)) and the Galois field represented in binary arithmetic, the subtraction operation (i.e. the inverse of addition) is the same as the addition operation. For convenience, the "+" symbol is used herein for this addition/subtraction operation, although a "-" symbol may be equivalently substituted for ease of understanding, as required.

IN THE ABSTRACT

Please cancel the present Abstract and substitute the rewritten Abstract attached.

IN THE CLAIMS

Please cancel claims 1-20 and add new claims 21-40 as follows:

21. (New) A program segment stored on a computer readable medium for cryptographically converting a digital input data block M into a digital output data block; said program segment comprising:

a program portion for merging a selected part M1 of said digital input data block M with a first digital key K1 to produce a data block B1 which non-linearly depends on said selected part M1 and said first digital key K1; and

a program portion for deriving said digital output block from said data block B1 and the remaining part of the digital input data block M, wherein said merging step is performed by executing a non-linear function g for non-linearly merging said selected part M1 and said first key K1 in a single step.

22. (New) A program segment as claimed in claim 21, comprising:

a program portion for splitting said digital input block into said selected part M1 and a second part M2 before executing said program portion for merging;

a program portion for executing a non-linear function g^{-1} to merge said second block M2 with a second key K2 in one step, producing a data block B2 as output; said non-linear function g^{-1} being the inverse of said non-linear function g; and

a program portion for forming combined data from data in said data block B1 and in said data block B2; said digital output block being derived from said combined data.

23. (New) A program segment as claimed in claim 21, wherein said program portion for merging comprises:

a program portion for splitting said selected part M1 in a first plurality n of sub-blocks $m_0,..,m_{n-1}$ of substantially equal length;

a program portion for splitting said first key K1 in said first plurality n of sub-keys $k_0,..,k_{n-1}$, substantially having equal length, the sub-key k_i corresponding to the sub-block m_i, for i = 0 to n-1;

a program portion for separately processing each of said sub-blocks m_i by executing for each of said sub-blocks m_i a same non-linear function h for non-linearly merging a sub-block b_i derived from said sub-block m_i with said corresponding sub-key k_i in one, sequentially inseparable step and producing said first plurality of output sub-blocks $h(b_i, k_i)$; and

a program portion for combining sub-blocks t_i derived from said first plurality of said output sub-blocks $h(b_i, k_i)$ to form said data block B1.

24. (New) A program segment as claimed in claim 22, wherein said program portion for executing said non-linear function g^{-1} comprises:

a program portion for splitting said second part M2 in said first plurality n of sub-blocks $m_n,..,m_{2n-1}$, substantially having equal length;

a program portion for splitting said key K2 in said first plurality n of sub-keys $k_n,..,k_{2n-1}$, substantially having equal length, the sub-key k_i corresponding to the sub-block m_i, for i = n to 2n-1;

a program portion for executing for each of said sub-blocks m_i a same non-linear function h^{-1} for non-linearly merging a sub-block b_i derived from said sub-block m_i with said corresponding sub-key k_i

and producing said first plurality of an output sub-block $h^{-1}(b_i, k_i)$; said function h^{-1} being the inverse of said function h; and

a program portion for combining sub-blocks t_i derived from said first plurality of output sub-blocks $h^{-1}(b_i, k_i)$ to form said data block B2.

25. (New) A program segment as claimed in claim 23, wherein said sub-block b_i is derived from said sub-block m_i by bit-wise adding a constant p_i to said sub-block m_i, said constant p_i substantially having equal length as said sub-block m_i.

26. (New) A program segment as claimed in claim 23, characterised in that said function $h(b_i,k_i)$ is defined by:

$h(b_i,k_i) = (b_i.k_i)^{-1}$, if $b_i \neq 0$, $k_i \neq 0$, and $b_i \neq k_i$

$h(b_i,k_i) = (k_i)^{-2}$, if $b_i = 0$

$h(b_i,k_i) = (b_i)^{-2}$, if $k_i = 0$

$h(b_i,k_i) = 0$, if $b_i = k_i$,

where the multiplication and inverse operations are predetermined Galois Field multiplication and inverse operations.

27. (New) A program segment as claimed in claim 26, wherein deriving said sub-blocks t_i from said output sub-blocks $h(b_i, k_i)$ comprises bit-wise adding a constant d_i to said output sub-block $h(b_i,k_i)$, said constant d_i substantially having equal length as said sub-block m_i.

28. (New) A program segment as claimed in claim 27, wherein deriving said sub-blocks t_i from said output sub-blocks $h(b_i, k_i)$ further comprises raising $h(b_i,k_i) \oplus d_i$ to a power 2^i, using said predetermined Galois Field multiplication.

29. (New) A program segment as claimed in claim 26, wherein deriving said sub-blocks t_i from said output sub-blocks $h(b_i, k_i)$ comprises raising said output sub-block $h(b_i,k_i)$ to a power 2^i, using said predetermined Galois Field (GF) multiplication.

30. (New) A program segment as claimed in claim 24, wherein said combined data is formed by:

swapping the sub-blocks t_i and t_{2n-1-i}, for i = 0 to n-1; and

concatenating the swapped sub-blocks.

31. (New) A program segment as claimed in claim 26, wherein said sub-block m_i comprises eight data bits, and wherein said multiplying of two elements b and c of $GF(2^8)$ comprises executing a series of multiplications and additions in $GF(2^4)$.

32. (New) A program segment as claimed in claim 31, wherein said multiplying of said two elements b and c comprises:

representing b as $a_0 + a_1.D$ and c as $a_2 + a_3.D$, where a_0, a_1, a_2 and a_3 are elements of $GF(2^4)$, and where D is an element of $GF(2^8)$ defined as a root of an irreducible polynomial $k(x) = x^2 + x + \beta$ over $GF(2^4)$, where β is an element of $GF(2^4)$; and

calculating $(a_0a_2 + a_1a_3\beta) + (a_1a_2 + a_0a_3 + a_1a_3).D$.

33. (New) A program segment as claimed in claim 32, wherein β is a root of an irreducible polynomial $h(x) = x^4 + x^3 + x^2 + x + 1$ over GF(2).

34. (New) A program segment as claimed in claim 26, wherein said sub-block m_i comprises eight data bits, and wherein calculating the inverse of an element b of $GF(2^8)$ comprises performing a series of calculations in $GF(2^4)$.

35. (New) A program segment as claimed in claim 34, wherein calculating the inverse of said element b comprises:

representing b as $a_0 + a_1.D$, where a_0 and a_1 are elements of $GF(2^4)$, and where D is an element of $GF(2^8)$ defined as a root of an irreducible polynomial $k(x) = x^2 + x + \beta$ over $GF(2^4)$, where β is an element of $GF(2^4)$; and

calculating $(a_0^2 + a_0a_1 + a_1^2\beta)^{-1}((a_0 + a_1) + a_1D)$.

36. (New) A processor for cryptographically converting a digital input block into a digital output block; said processor comprising:

a first input for obtaining said digital input block;

a second input for obtaining a first key K1; and

a cryptographic processing portion arranged to convert the digital input block into the digital output block by executing a non-linear function g for non-linearly merging said selected part M1 and said first key K1 in one step and producing a data block B1 which non-linearly depends on said selected part M1 and said first key K1, where a selected part of said digital output block is derived from said data block B1.

37. (New) A processor as claimed in claim 36, wherein said processor comprises a third input for obtaining a second key K2, and wherein said processor is arranged to:

split said digital input block into said selected part M1 and a second part M2 before performing said merging;

perform a non-linear function g^{-1} to merge said second block M2 with said second key K2 in one step, producing a data block B2 as output; said non-linear function g^{-1} being the inverse of said non-linear function g; and combine data from data in said data block B1 and in said data block B2; said digital output block being derived from said combined data.

38. (New) A processor as claimed in claim 36, wherein said merging comprises:

splitting said selected part M1 in a first plurality n of sub-blocks $m_0,..,m_{n-1}$ of substantially equal length;

splitting said first key K1 in said first plurality n of sub-keys $k_0,..,k_{n-1}$, substantially having equal length, the sub-key k_i corresponding to the sub-block m_i, for i = 0 to n-1; and

separately processing each of said sub-blocks m_i by executing for each of said sub-blocks m_i a same non-linear function h for non-linearly merging a sub-block b_i derived from said sub-block m_i with said corresponding sub-key k_i in one, sequentially inseparable step and producing said first plurality of output sub-blocks $h(b_i, k_i)$; and

combining sub-blocks t_i derived from said first plurality of said output sub-blocks $h(b_i, k_i)$ to form said data block B1.

39. (New) A processor as claimed in claim 38, wherein said function $h(b_i,k_i)$ is defined by:

$h(b_i,k_i) = (b_i.k_i)^{-1}$, if $b_i \neq 0$, $k_i \neq 0$, and $b_i \neq k_i$

$h(b_i,k_i) = (k_i)^{-2}$, if $b_i = 0$

$h(b_i,k_i) = (b_i)^{-2}$, if $k_i = 0$

$h(b_i,k_i) = 0$, if $b_i = k_i$,

where the multiplication and inverse operations are predetermined Galois Field multiplication and inverse operations.

40. (New) A processor as claimed in claim 19, wherein said sub-block m_i comprises eight data bits, and wherein said multiplying of two elements b and c of $GF(2^8)$ comprises:

representing b as $a_0 + a_1.D$ and c as $a_2 + a_3.D$, where a_0, a_1, a_2 and a_3 are elements of $GF(2^4)$, and where D is an element of $GF(2^8)$ defined as a root of an irreducible polynomial $k(x) = x^2 + x + \beta$ over $GF(2^4)$, where β is an element of $GF(2^4)$; and

calculating $(a_0a_2 + a_1a_3\beta) + (a_1a_2 + a_0a_3 + a_1a_3).D$;

and wherein calculating the inverse of an element b of $GF(2^8)$ comprises calculating $(a_0^2 + a_0a_1 + a_1^2\beta)^{-1}((a_0 + a_1) + a_1D)$.

REMARKS

This Amendment is being filed to continue prosecution of Claims cancelled without prejudice in a priority application and in response to the Advisory Action mailed March 20, 2001 and the Final Office Action mailed September 12, 2000. Reconsideration and allowance of the application in view of the amendments made above and the remarks to follow are respectfully requested.

Claims 21-40 are pending in this application of which Claims 21 and 36 are independent claims.

In the outstanding rejection, the claims were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,488,661 to Matsui ("Matsui") in view of U.S. Patent No. 5,398,284 to Koopman ("Koopman").

The Applicant specifically claims a program (claim 21) and processor (claim 36), wherein the merging step is performed by executing a ***non-linear function*** for non-linearly merging a select part of the plaintext with a first key in ***a single step***. The Applicant maintains that both Matsui and Koopman present a ***linear*** merging, and Koopman presents a ***multi-step*** process that augments the linear merging with a non-linear operation.

The Office Action asserts that Matsui and Koopman present a non-linear process. The Applicant has repeatedly and continuously maintained that the difference between Applicant's claimed invention and Matsui and Koopman is the fact that the Applicant teaches and claims the merging of a select part of the plaintext data with the key in a ***single non-linear step***.

An "Introduction to Switching Theory and Logical Design", by Hill and Peterson, published 1968, presents a definition of a linear function in the context of a switching system as would be readily understood by a person of ordinary skill in the art, following on page 420, it states that:

> "A linear switching function is a switching function, which may be realized using only AND gates and exclusive-or gates."

The above is true because in a switching system (i.e. a two-value, 0-1, system, which is conventionally termed a "digital" system), the "addition" function corresponds to an exclusive-or function, and the "multiplication" function corresponds to an AND function.

The DES algorithm, Matsui (item 12 in Matsui's FIG. 1), and Koopman (items 12 and 14 in FIG. 1) each use an exclusive-or function to merge the plaintext data with the key. That is, DES, Matsui, and Koopman each use a linear function to merge the plaintext data with the key.

In "Applied Cryptography", by Schneier, published in 1996, Schneier notes this linear-then-nonlinear sequential process in DES:

> "The S-box substitution is the critical step in DES. The algorithm's other steps ***are linear*** and easy to analyze. The S-boxes are ***nonlinear*** and, more than anything else, give DES its security."

In DES, the "other steps" include the merging of the select part of the plaintext with the key, via an exclusive-or function.

Matsui specifically illustrates that a select portion of the plaintext data 3 is merged with the output of the "f" block 9 via an exclusive-or gate 12. By definition, this is a linear operation.

In the Office Action of 16 September 1999, an argument is presented for demonstrating that Matsui's process is non-linear. The Applicant respectfully notes that the presentation is flawed. Following the presented argument, any and all two-input functions are non-linear. That is, the Argument uses an undefined function

"L" in the "proof", and goes on to demonstrate that, regardless of the particular function "L", "L(P1 + P2) = L(P1) + L(P2) + 2M". That is, even if the function "L" is linear, such as a simple addition function, the derivation **mistakenly leads to a result** that a simple addition function is non-linear, which clearly is not true. Further, this error is readily apparent to any person skilled in the art.

Koopman uses a bitwise shifting and exclusive-or operation that "can be viewed as a ***multiplication*** operation between the register and mask in the Galois Field GF(2^n). This operation is, in effect, a convolution operation" (Koopman, column 4, lines 43-47). To add a non-linearity to this linear (multiplication) process, Koopman halts the convolution after a 'secret' number of multiplications, and a nonlinear (without carry) Integer Ring operation is performed (Koopman, column 4, lines 51-58, and column 5, lines 35-40).

The Applicant respectfully maintains that both Matsui and Koopman teach a linear merging of the select part of the plaintext with the key. The Applicant further maintains that neither Matsui, nor Koopman, individually or collectively, teach or suggest merging a select part of the plaintext with a key via a single-step non-linear function, as specifically required by each of the currently pending claims. Accordingly, the Applicant respectfully request that claims 21-40 be allowed.

Early and favorable action is earnestly solicited.

Respectfully submitted,

By ______________________

Gregory L. Thorne, Reg. 39,398
Senior Patent Counsel
(914) 333-9665
August 8, 2001

APPENDIX

AMENDED SPECIFICATION

Page 1, in the paragraph beginning on line 1, change as follows:

FIELD OF THE INVENTION

The invention relates to a method for converting a digital input block into a digital output block; said conversion comprising the step of merging a selected part M1 of ~~said~~ the digital input block with a first key K1 and producing a data block B1 which non-linearly depends on ~~said~~ the selected part M1 and ~~said~~ the first key K1, and where a selected part of ~~said~~ the digital output block is derived from ~~said~~ the data block B1.

Page 1, in the paragraph beginning on line 6, change as follows:

The invention further relates to an apparatus for cryptographically converting a digital input block into a digital output block; ~~said~~ the apparatus comprising first input means for ~~obtaining said~~ supplying the digital input block; second input means ~~for obtaining~~ for supplying a first key K1; cryptographic processing means for converting the digital input block into the digital output block; ~~said~~ such conversion comprising merging a selected part M1 of ~~said~~ the digital input block with ~~said~~ the first key K1 and producing a data block B1 which non-linearly depends on ~~said~~ the selected part M1 and ~~said~~ the first key K1, and where a selected part of ~~said~~ the digital output block is derived from ~~said~~ the data block B1; and output means for outputting ~~said~~ the digital output block.

Page 1, in the paragraph beginning on line 15, change as follows:

BACKGROUND OF THE INVENTION

The Data Encryption Standard (DES) of the National Bureau of Standard [FIPS publication 46, 1977 January 15] describes a widely used algorithm for converting a digital input block into a digital output block. Such an algorithm is generally referred to as a block cipher. The DES algorithm is used for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting converts intelligible data, referred to as plaintext, into an unintelligible form, referred to as ciphertext. Decrypting the ciphertext converts the data back to its original form. In the so-called electronic code book mode, DES is used to encrypt blocks of 64 bits of plaintext into corresponding blocks of 64 bits of ciphertext. In this mode, the encryption uses keys which are derived from a 64 bit key, of which 56 bits may be freely selected. Figure 1 shows the overall structure of DES during encrypting. In the encrypting computation, the input (64 bit plaintext) is first permuted ~~from 64 bits into 64 bits~~ using a 64 bit fixed permutation IP. The result is split into 32 left bits L_0 and 32 right bits R_0.

The right bits are transformed using a cipher function $f(R_0,K_1)$, where K_1 is a sub-key. The result $f(R_0,K_1)$ is added (bit-wise modulo 2) to the left bits, followed by interchanging the two resulting 32 bit blocks L_0 □ $f(R_0,K_1)$ and R_0. This procedure is continued iteratively for a total of 16 rounds. At the end of the last round the inverse permutation of the initial permutation IP is applied.

Page 3, in the paragraph beginning on line 6, change as follows:

SUMMARY OF THE INVENTION

It is an object of the invention to provide a cryptographic method and apparatus of the kind set forth which is more robust against cryptanalytic attacks.

Page 3, in the paragraph beginning on line 9, change as follows:

To achieve this object, the cryptographic method according to the invention is characterised in that ~~said merging~~ the step of merging the data and the key is performed by executing a non-linear function g for non-linearly merging said selected part M1 of the data and said first key K1 in one, sequentially inseparable step. In the DES system, as shown in figure 2, in a first processing step the R data is bit-wise added to the key, followed by a second processing step of non-linearly processing the result (S-boxes). According to the invention, an algorithm is used which non-linearly merges data with a key in one step (i.e. one, sequentially inseparable step). As such, adding the key bits to the data is an integrated part of the non-linear operation, making the system more immune against modern attacks, such as differential cryptanalysis.

Page 3, in the paragraph beginning on line 19, change as follows:

In an embodiment of the method according to the invention ~~as defined in the dependent claim 2~~, in each round both parts of the digital input block are processed, giving a better encryption result than for conventional Feistel ciphers, such as DES, where during each round only half of the digital input block is being processed. To ensure that the same system can be used for both encryption and decryption, one part of the data is processed using an operation g, whereas the other half is processed using the inverse operation g^{-1}. Using this scheme, decrypting is performed by using the same system but supplying the keys in reverse order to the rounds (during decryption the first non-linear step is supplied with the key which, during encryption, was supplied to the last non-linear step, etc). Compared to a conventional implementation of a Feistel cipher with twice as many rounds, the system according to the invention is faster.

Page 3, in the paragraph beginning on line 30, change as follows:

The measure ~~as defined in the dependent claim 3, wherein~~ of splitting a relatively large data block and key, of for instance 64 bits, ~~are split~~ into smaller sub-blocks and sub-keys simplifies real-time non-linear processing.

Page 3, in the paragraph beginning on line 33, change as follows:

In an embodiment of the method according to the invention ~~as defined in the dependent claim 5~~, a constant is used to enhance the quality of the encryption. Advantageously, the constant is predetermined per system, forming, for instance, a customer-specific constant. Alternatively, the constant is generated using a pseudo-random generator.

Page 4, in the paragraph beginning on line 3, change as follows:

The ~~measure defined in dependent claim 6~~ invention provides a way for non-linearly merging the data sub-block and the sub-key in one step. Additionally, different inputs all result in different outputs. This increases the immunity of the system against cryptanalytic attacks, compared to DES where the non-linear operation reduces the 6-bit input sub-block to a 4-bit output sub-block, implying that the same output is produced for four different inputs.

Page 4, in the paragraph beginning on line 8, change as follows:

In an embodiment of the method according to the invention ~~as defined in the dependent claim 7~~ a constant is used to enhance the quality of the encryption. Advantageously, the constant is predetermined per system, forming, for instance, a customer-specific constant. Alternatively, the constant is generated using a pseudo-random generator.

Page 4, delete the entire paragraph beginning on line 12.

Page 4, in the paragraph beginning on line 14, change as follows:

In an embodiment of the method according to the invention ~~as defined in the dependent claim 10~~ individual sub-blocks corresponding to different parts of the digital input block are swapped to improve the quality of the encryption.

Page 4, in the paragraph beginning on line 20, change as follows:

~~The measure as defined in the dependent claim 11~~ Another embodiment has the advantage of reducing the multiplication in GF(2^8) to operations in GF(2^4), making it possible to achieve a simpler or more cost-effective implementation.

Page 4, in the paragraph beginning on line 23, change as follows:

~~The measure defined in the dependent claim 12 gives an effective way of reducing the~~ The multiplication in GF(2^8) may be reduced to operations in GF(2^4).

Page 4, in the paragraph beginning on line 28, change as follows:

An embodiment of the method according to the invention is characterised in that calculating the inverse ~~of~~ b in an element of GF(2^8) comprises performing a series of calculations in GF(2^4). By reducing the inverse operation in GF(2^8) to operations in GF(2^4) a simpler or more-cost effective implementation can be achieved.

Page 5, in the paragraph beginning on line 13, change as follows:

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows the processing steps for the DES system,

Figure 2 illustrates details of merging the data with the key and the non-linear operation in DES,

Figure 3 illustrates details of the key calculation in DES,

Figure 4 shows a block diagram of the cryptographic apparatus of the invention,

Figure 5 illustrates separate processing of two parts of the digital input block,

Figure 6 illustrates processing of a part of the digital input block in the form of sub-blocks,

Figure 7 illustrates processing of two parts in the form of sub-blocks, and

Figure 8 shows an overall encryption system.

Page 5, in the paragraph beginning on line 25, change as follows:

DETAILED DESCRIPTION OF THE INVENTION

Figure 4 shows a block diagram of the cryptographic apparatus 400 according to the invention. For the purpose of explaining the invention, the system is described in the electronic code book mode. Persons skilled in the art will be able to use the system in other modes as well.The apparatus 400 comprises first input means 410 for ~~obtaining~~ providing a digital input block M. The digital input block M may be any suitable size. Preferably, M is sufficiently large, for instance 128 bits, to obtain a reasonably secure encryption result. The apparatus 400 further comprises cryptographic processing means 420 for converting the digital input block into a digital output block. Advantageously, the digital output block has substantially equal length as the digital input block. The apparatus 400 comprises output means 430 for outputting the digital output block. Basically, the cryptographic processing means 420 converts the digital input block M into the digital output block by merging a selected part M1 of the digital input block M with a first key K1, producing a data block B1 which non-linearly depends on M1 and K1. The merging is performed in one, sequentially inseparable step. The digital output block is derived from B1 and the remaining part of M, which is not part of M1. To obtain the first key K1, the cryptographic apparatus 400 comprises second input ~~means~~ block 440. As will be described in more details below, a second part M2 of the digital input block may be non-linearly merged with a second key K2, preferably, using an operation inverse to the operation for merging M1 and K1, producing a data block B2. In this case, the digital output block also depends on B2. To obtain the second key K2, the cryptographic apparatus 400 comprises third input ~~means~~ block 450.

Page 6, in the paragraph beginning on line 22, change as follows:

~~In the remainder of the document details~~ Details of the cryptographic conversion ~~are given~~ process will now be described for encrypting blocks of 128 bits of plaintext into corresponding blocks of 128 bits of ciphertext. Persons skilled in the art will be able to use the system for other block sizes as well. Data sizes shown in the Figures are given for reasons of clarity and should be treated as examples only. The description focuses on the non-linear processing of the data and the merging of the key with the data as performed in one round. As such the invention can be applied in a system as shown in Figure 1, comprising multiple rounds and also including a linear operation on the data block in each round.

Page 10, in the paragraph beginning on line 19, change as follows:

In principle, for the invention any multiplication in GF(2^8) may be used. An example of a VLSI implementation of multiplications in GF(2^m) is given in [P. A. Scott, "A fast VLSI multiplier for

GF(2^m)", IEEE Journal on selected areas in communications, Vol. SAC-4, No. 1, January 1986, pages 62-66]. Advantageously, the following mechanism is used to reduce the multiplication in GF(2^8) to a series of multiplications and additions in GF(2^4). As is known in the art, in finite fields with a characteristic of 2 (e.g. GF(2^n)) and the Galois field represented in binary arithmetic, the subtraction operation (i.e. the inverse of addition) is the same as the addition operation. For convenience, the "+" symbol is used herein for this addition/subtraction operation, although a "-" symbol may be equivalently substituted for ease of understanding, as required.

ABSTRACT OF THE DISCLOSURE

A method and apparatus for cryptographically converting a digital input data block into a digital output data block. The apparatus has an input for supplying the input data block and a further input for supplying a code conversion digital key K1. Cryptographic processing merges a selected part M1 of the digital input data block with the key K1 to produce a data block B1 that is non-linearly dependent on M1 and K1. The merging is performed in one sequentially inseparable step. The digital output block is derived from a selected part of the data block B1.